GUIDELINES ON ANONYMITY AND CONFIDENTIALITY IN RESEARCH

Development Date: May 2015
Revised Date: November 2017

Table of Contents

1. Purpose

The purpose of this guideline is to provide researchers with information on anonymity and confidentiality with respect to research involving human participants. It also lays out three special circumstances where there may be limits to respecting the privacy and confidentiality of research participants.

2. Background and Key Terms

All researchers conducting studies involving humans have a duty to protect the privacy of their participants. This entails that researchers take steps to properly safeguard sensitive and personal information that participants would not reasonably want to disclose to others or make public. There are two main ways to ensure that the privacy of participants is being respected: (1) by conducting anonymous research, and (2) by conducting confidential research.

Anonymous Research means that at no time will the researcher or anyone associated with the project know the identity of the participants. In anonymous research, the information collected does not contain any identifiable information, and the risk of being able to attribute data to particular individuals is low (p. 59). *[i]

Confidential Research means that proper safeguards are in place to protect the privacy of participants and their information from unauthorized access, use, disclosure, modification, loss, and theft (p. 202).

Anonymized Information is information that is irrevocably stripped of all direct identifiers – e.g., name, social insurance number, health number, etc., – and where both the risk of re-identification from remaining indirect identifiers is low, and where no codes exist that could allow for future re-linkage (p. 206). When information is anonymized, even the researcher will not be able to link data to participants.

De-Identified Data is data provided to the researcher in de-identified form and the existing key code is accessible only to a custodian or trusted third party who is independent of the researcher (p.59).

Identifiable information is information that may reasonably be expected to identify an individual alone or in combination with other available information (p. 205). This includes both direct and indirect identifying information. **Direct identifying information** identifies a specific individual through identifiers, such as a name, social insurance number, personal health number, etc. **Indirect Identifying information** is information that can reasonably be expected to identify an individual through a combination of indirect identifiers, such as someone's date of birth, place of residence, unique characteristics, and so on (p. 206).

Coded Information is information that has been stripped of all direct identifiers and replaced with a code. This code can then be used to attribute specific data to particular participants (p. 206).

3. Managing Confidentiality

All individuals conducting research involving human participants have a duty to keep their participants' information confidential (p.58). This duty entails that researchers implement safeguards to protect the confidentiality of their participants throughout all stages of the research cycle. This includes the following stages:

- Recruitment;
- The initial collection of information/data;
- The use of and analysis of the information/data collected;
- The dissemination of the findings;
- The storage and retention of information; and
- The disposal of records or devices on which information is stored.

Precisely how researchers should go about incorporating safeguards at these various stages of the research cycle will vary based on the nature of their projects. Below are f types of safeguards that may be put into place in order to help protect the confidentiality and privacy of research participants: physical safeguards, administrative safeguards, technical safeguards, and research design safeguards.

I. **Physical safeguards** are measures that secure the location of private and sensitive information from unauthorized personnel. Examples of physical safeguards include locked filing cabinets, secluded interview rooms, private offices, storing information away from public, and easily accessible areas, etc. (p. 63).

II. **Administrative safeguards** are measures that protect the privacy of participants' information by clearly delineating who does and who does not have access to participants' information, and in what ways (p. 63). Typically, the greater the number of individuals that have access to private and confidential information, the more difficult it is to protect the privacy and confidentiality of participants' information. As a result, a minimum number of research staff, all of whom must be instructed about confidentiality requirements, should have access to participants' data.

III. **Technical safeguards** are technological measures that protect the privacy of participants. These include the use of computer passwords, firewalls, anti-virus software, encryption and other measures that protect data from unauthorized individuals, loss, theft or modification (p.

63). Typically, all electronic data should be password protected, and based on the sensitivity of the information, also encrypted.

IV. **Research design safeguards** are measures intrinsic to the research design of a project that help protect the privacy of research participants. These include anonymizing information, transcribing raw data as soon as possible, storing de-identified data separately from coding lists, shredding all hard copies with sensitive information as soon as feasible, and so on.

It is important to note that the onus is on researchers to demonstrate to the Research Ethics Board (REB) that the confidentiality of research participants is being adequately safeguarded and protected. The safeguards implemented by researchers to protect the privacy and confidentiality of research participants should be clearly stated in the section entitled "Privacy and Confidentiality" in the online application and on the consent form.

4. The Limits of Privacy and Confidentiality: Special Circumstances

There are three circumstances where the duty to protect the privacy and confidentiality of participants' information **may** be outweighed by other competing factors: (I) where adopting measures to protect the privacy of participants is inimical to the integrity of the research design; (II) where researchers are under a legal responsibility or a duty to report participants' information to the authorities; and (III) where respecting the confidentiality of participants' information undermines the autonomy of research participants.

I. Research Inimical to Protecting the Confidentiality of Participants' Information

Researchers whose projects are inimical to protecting the confidentiality of participants' information – such as large focus groups – may be unable to ensure that their participants' information is kept confidential. In cases such as this, the researcher must disclose the privacy and confidentiality risks to potential participants inherent in their participation to the REB, and to participants in the consent form, and, if possible, also in person.

For example, in the case of a focus group, a researcher should write something like the following on the consent form: "While I, the researcher, will respect the confidentiality of all participant's information, I cannot promise or ensure that other participants will do the same. I will, however, ask all participants in the study to respect the confidentiality of all participants." And, at the start of the focus group, a researcher could begin by stating something like the following: "Given that we will be discussing personal and sensitive information, I ask you all not to share or disclose anything mentioned here with others. I will respect the confidentiality of all participants' information shared here in this focus group, and I ask all of you to do the same."

II. Legal Necessity & Duty to Report

Researchers may be required to disclose confidential information regarding their participants to the appropriate authorities when required by law or if there is a special duty to report. Below are three examples of cases where there is a duty to report that stem from either legal necessity or professional obligation.

Example 1: Individuals conducting research involving children under 16 years of age (or under 17 years of age if the child is under a child protection order) are required by law to report to the proper authorities any suspicions of child neglect or abuse that they may come across during the duration of their research.

Example 2: Researchers who are also a part of certain professional associations may be required by oath and/or by law to breach confidentiality in the event that they find out that their participants pose an imminent harm to themselves or others.

Example 3: Researchers may also be required by law to share participants' confidential information with various government agencies, such as Health Canada, the U.S. Food and Drug Administration, or national security agencies, in the event that a subpoena is received.

III. Respecting the Autonomy of Research Participants

While all researchers have a duty to ensure that their participants' information is kept confidential, in some cases, researchers may come across interested participants who wish to receive recognition for their contributions to a project or have their information made known in various ways. In some of these cases, respecting the autonomy and personhood of participants requires researchers to honour their participants' wishes. In these cases, researchers have a duty to communicate to their participants any new confidentiality and privacy risks associated with their participation.

In order to ensure that these new risks are properly mitigated and minimized, researchers need to request to reopen their protocol and make an amendment that reflects the new privacy and confidentiality risks, and how these risks will be managed. Researchers will also have to revise their consent forms accordingly. Before researchers share participants' confidential information or agree to share it, approval must be obtained from the REB.

N.B. The onus is on researchers to be aware of the likely ways that their research design may undermine their ability to protect participants' confidential information. It is important that in all research designs where breaches of confidentiality may occur, the risks associated with such breaches are clearly communicated to research participants, so that they can make an informed choice as to whether they would like – or not like – to participate in the project.

5. Confidentiality Breach

No matter how carefully crafted your safeguards may have initially been, and no matter how closely you follow your safeguards in order to keep your participants' information confidential, breaches of confidentiality can occur. For example, a locked cabinet storing sensitive information may be broken into, private information stored online that is password protected and encrypted may be hacked and retrieved using a deciphering code, or a research assistant may accidentally disclose private and confidential information to a friend.

Regardless of how the confidentiality breach occurs, it is imperative that researchers email the Chair of the Research Ethics Board **as soon as possible** to outline the details of the confidentiality breach. This email should be directed to rebchair@torontomu.ca. This should be followed within 72 hours by the completion and submission of an Adverse/Unanticipated Event Report. You can also, at any time, call the REB Office 416-979-5042 if you require more urgent advice or guidance.

The REB will advise the researcher on how best to manage, minimize, and mitigate any negative effects as a result of the confidentiality breach, and will help the researcher in developing further measures that such a breach does not happen again. In some cases, restitution may be required by those negatively affected as a result of the confidentiality breach.

---

[i] *All page number references refer to the online version of the Tri-Council Policy Statement (TCPS 2, 2014).

Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council of Canada, *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans*, *December 2014*.